SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2026
ORGANIZATION AND MANAGEMENT SERIES NO. 250

ORGANIZATIONAL CAPABILITIES IN THE FIELD OF CYBERSECURITY FOR IMPORTANT ENTITIES UNDER THE NIS2 DIRECTIVE. AN ANALYSIS OF SELECTED MANAGEMENT CHALLENGES. THE POLISH PERSPECTIVE

Łukasz DOMŻAŁ-DRZEWICKI

Lublin University of Technology; d639@pollub.edu.pl, ORCID: 0009-0003-7314-8348

Purpose: The purpose of this paper is to identify and analyse key management challenges related to building organizational capabilities in important entities in Poland, which are subject to the NIS2 Directive and its national implementation.
Design/methodology/approach: The research is based on qualitative analysis of regulatory documents and industry literature. The study uses desk research of EU and Polish legal acts, complemented by a review of standards and best practices and recent academic publications on cybersecurity management and organizational resilience. On this basis, a conceptual framework of three challenge groups is developed: identification, organizational and operational, with a focus on the Polish interpretation of NIS2 for important entities.
Findings: The analysis shows that effective NIS2 implementation requires capabilities in three interrelated dimensions. Identification challenges concern status assessment, sectoral qualification and designation of systems covered by ISMS. Organizational challenges involve responsibility models, competence structures, and governance over internal and outsourced cybersecurity, including ICT supply chains. Operational challenges include monitoring, incident reporting, documentation and cooperation with authorities under time pressure, affecting continuity and costs.
Research limitations/implications: The paper is conceptual and based on secondary sources; it does not include empirical verification at the level of individual organizations. Future research should involve empirical studies of important entities in different sectors together with quantitative assessment of the impact of NIS2 on organizational maturity and costs.
Practical implications: The results provide a structured lens for managers and policymakers to plan NIS2 implementation as a long-term management process rather than a one-off compliance project.
Social implications: By strengthening organizational capabilities of important entities in defined sectors, the implementation of NIS2 contributes to higher digital resilience of the state and economy. This may translate into improved continuity of essential services, greater protection of citizens and increased trust in public and private institutions.
Originality/value: The paper offers a management-oriented interpretation of NIS2 and national act focused specifically on important entities. It proposes a clear, three-part framework of challenges that links legal requirements with organizational practice, providing added value for both researchers and practitioners in cybersecurity governance.
Keywords: NIS2, important entity, risk management, uKSC, organizational capabilities.
Category of the paper: Research paper.

1. Introduction

The current development momentum of both the economy and public administration in Poland and Europe is driving an increasing dependence on complex, interdependent information and communication technology (ICT) systems. This reality objectively improves quality of life, offering hope for multi-domain economic development and the elimination of various forms of social and civilizational exclusion. At the same time, however, it multiplies new and deepens existing problems associated with the consequences of cybersecurity incidents, ranging from disruptions to organizational continuity and supply chains, through threats to citizen and national security, to the broader destabilization of the economic system. One measure of the scale of this phenomenon is the fact that in 2025 alone, Polish CSIRT teams recorded 272,941 cybersecurity incident reports. The intensity and professionalization of cybersecurity events is systematically increasing. Their perpetrators include both organized criminal groups and state-sponsored actors, increasingly targeting critical infrastructure and supply chains. Industry 5.0, along with the current expansion of artificial intelligence-based solutions, means that cybersecurity management is ceasing to be an exclusively technical domain and is becoming a pillar of organizational resilience and a foundation of stakeholder trust (Dacko-Pikiewicz, Szczepańska-Woszczyna, Lis, 2025; ENISA, 2023; Hubbard, Seiersen, 2024; Ministerstwo Cyfryzacji 2026; NIST, 2018).

The European Union's (EU) response to the growing digital risks is the NIS2 Directive (Directive (EU) 2022/2555), establishing a legal framework for key and important entities operating in 18 sectors designated in Annexes I and II of the aforementioned directive, extending the scope of obligations in risk management, incident reporting, and supervision. In Poland, the transposition of the NIS2 Directive is ensured by the Act of 23 January 2026 amending the Act on the National Cybersecurity System and certain other acts (uKSC), amending the parent act of 5 July 2018. The amendment introduces principles and obligations concerning the organization of the national cybersecurity system, defining requirements for important entities in the areas of risk management, incident reporting, and maintaining digital resilience (UE L 333, 2022; Dz.U.2026 poz. 252; Ministerstwo Cyfryzacji, 2026).

NIS2 and the uKSC operate within the broader EU regulatory ecosystem, encompassing among other GDPR, DORA, and the AI Act, which together create a multi-layered framework of accountability for digital security. DORA (Regulation (EU) 2022/2554), as a sectoral regulation for the financial sector, consolidates requirements for ICT risk management, incident reporting, resilience testing, and ICT provider oversight, assigning full responsibility for ICT risk to the management body, thereby reinforcing ongoing board engagement and investment levels, a logic consistent with the managerial accountability regime under NIS2. The AI Act (Regulation (EU) 2024/1689) introduces a risk-based AI governance system, prohibiting unacceptable practices, defining requirements for high-risk systems, and establishing

transparency obligations; for key and important entities, this requires ensuring the cybersecurity and resilience of AI systems throughout their lifecycle and continuous improvement of security processes by operators and providers, increasing managerial accountability across the organizational ecosystem (Rozporządzenie (UE) 2024/1689; Rozporządzenie (UE) 2022/2554; Dyrektywa (UE) 2022/2555).

Organizational cybersecurity management has long rested on widely accepted frameworks. Including ISO/IEC 27001, NIST CSF, OWASP, and MITRE ATT&CK, to which NIS2 refers. The Directive is therefore primarily an enforcement mechanism rather than a creative one: codifying in EU law what the cybersecurity community has developed and recommended for years, while bringing within its scope numerous new important entities that have often for economic, cultural, or organizational reasons limited their investments in security, resilience, supply chain security, and employee education. It imposes on them the obligation of genuine, documented implementation of these practices under penalty of sanctions. The ENISA NIS Investments 2023 report indicates that the main barriers to implementing cybersecurity best practices in entities include, among others, competence shortages, limited leadership, and weak security culture. Manifested in difficulties recruiting qualified specialists, insufficient budgets, and low levels of participation in information-sharing initiatives. Additionally, limited management engagement hinders the implementation of necessary practices and procedures. In response to these challenges, the NIS2 Directive introduces personal liability for managers, mandatory board training, and a requirement to document security plans and procedures, in order to genuinely raise the level of competence and engagement throughout the organization (Dz.U. 2026, poz. 252; ENISA, 2023; Ministerstwo Cyfryzacji, 2026; NIST, 2018; OWASP, 2021).

The aim of this article is to identify selected management challenges associated with building organizational capabilities in important entities in Poland falling within the scope of the NIS2 Directive and the uKSC. This leads to the following research question: what key management challenges do important entities face when building organizational capabilities in the field of cybersecurity in accordance with the requirements of the NIS2 Directive and the Polish transposition?

The study adopts a qualitative, conceptual research design based on regulatory desk research and a literature review, described in Section 2.

2. Research Methodology

This paper adopts a qualitative, conceptual research design based on secondary data analysis. The study does not include empirical verification at the level of individual organizations. Instead, it draws on regulatory documents, institutional guidance, normative

frameworks, and academic literature to develop a structured analytical framework of management challenges. Source selection was guided by four criteria:

1. the regulatory relevance of sources directly shaping cybersecurity obligations for important entities under EU and Polish law, including the NIS2 Directive, the uKSC amendment, GDPR, DORA, the AI Act, and the Cyber Resilience Act,
2. the institutional authority of guidance and reports published by recognized bodies, such as the Ministry of Digitization, ENISA, NIST, and OWASP,
3. the actuality of publications published or updated following the adoption of the NIS2 Directive and its transposition into Polish law in 2026, and
4. the topical relevance of academic literature on cybersecurity management, organizational resilience, and governance, with particular attention to issues related to NIS2 implementation.

The analytical procedure followed three sequential steps. First, applicable legal acts and the Ministry of Digitization's Q&A implementation guide were analyzed to identify the core obligations imposed on important entities. Second, relevant normative frameworks (NIST CSF, OWASP) and academic publications were reviewed to contextualize these obligations within broader cybersecurity governance concepts. Third, the findings were synthesized into a three-dimensional framework of challenges: identification, organizational, and operational. This structure reflects the sequential logic of NIS2 implementation. From determining regulatory status, through building internal capabilities, to maintaining ongoing compliance, and maps directly onto the main obligation clusters defined in the uKSC amendment. The framework was validated through triangulation of regulatory sources, institutional guidance, and academic literature to ensure internal consistency and completeness. The analyzed sources were coded according to clusters of responsibilities derived from NIS2/uKSC: status identification, management and accountability, competencies and outsourcing, risk management, incident reporting, monitoring, documentation, and cooperation with authorities. These codes were then grouped into three overarching analytical categories: identification, organizational and operational challenges. Since the study is conceptual in nature and relies on secondary sources, coding was used as a technique for analytical structuring rather than as a procedure for quantitative content analysis (Dyrektywa (UE) 2022/2555; Dz.U. 2026, poz. 252; ENISA, 2023; NIST, 2018).

3. NIS2 and the Polish transposition: selected scope, important entities, and the logic of obligations

The NIS2 Directive and its polish implementation assume that cybersecurity is not merely a technological issue, but rather the foundation for ensuring the uninterrupted provision of services of social and economic significance. The recitals to the Directive state that the growing number, scale, sophistication, and impact of incidents necessitate the creation of coordinated regulatory frameworks and the definition of a catalogue of sectors and activities subject to cybersecurity and general resilience obligations. These regulations focus not so much on specifying particular protective tools as on the organization's capacity for comprehensive risk management, incident response, and the maintenance of high operational resilience. In the Polish transposition, this logic is reflected in the departure from the earlier model based on operators of essential services and its replacement with the categories of key entities and important entities. The amendment to the Act on the National Cybersecurity System explicitly states that it transposes the NIS2 Directive into domestic law (Dyrektywa (UE) 2022/2555; Dz.U. 2026, poz. 252).

Within the scope of this article, particular attention is devoted to the group of entities referred to as important entities. In accordance with Article 5(2) of the uKSC amendment, both general qualification criteria and exceptions are defined. In practice, this category refers primarily to entities operating in the sectors specified in Annex 2 to the Act, including: postal services, nuclear energy investments, waste management, production, manufacture and distribution of chemicals, production, processing and distribution of food, manufacturing, digital service providers, scientific research, and public entities. This arrangement confirms that the status of an important entity results from a combination of statutory criteria and assignment to sectors deemed significant from the perspective of the digital resilience of the state and economy. The presented arrangement indicates that obtaining the status of an important entity is not dependent solely on the size of the organization, but results from a combination of criteria concerning size, sector membership, and for certain cases a specific designation indicated in the Act (Dyrektywa (UE) 2022/2555; Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The manner of identifying this category of entities is of significant importance. The Polish model is based primarily on self-identification that is, the obligation of an organization to independently establish its own size, scope of activities, and to relate these elements to the uKSC and its annexes. According to a document published by the Ministry of Digitization, administrative decisions are applied exceptionally rather than as a rule. This concerns special cases where the authority responsible for cybersecurity may decide to bring within the scope of the Act an entity that does not meet the typical criteria but is significant from the perspective of state security, continuity of services, or existing risk (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

From the perspective of building systemic resilience, the substantive obligations of key and important entities are in principle identical. The difference concerns primarily the model of supervision and audit. The Ministry of Digitization document clearly indicates that supervision of key entities is of an ex ante nature, while supervision of important entities is ex post. Key entities conduct audits every 3 years and at the request of the competent cybersecurity authority, whereas important entities conduct audits exclusively at the request of that authority. The difference between the two categories does not result from different security requirements but from a different degree of supervision and enforcement of those obligations (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The fundamental idea underlying the obligations arising from the regulations is to ensure a uniform minimum level of organizational resilience for all entities covered by the Act. The most important is actual obligation to create and maintain an information security management system around the information systems used by entities. In accordance with Article 8 of the Act, such system must enable:

- regular risk assessment and effective risk management,
- implementation of adequate and proportionate technical and organizational measures, taking into account current knowledge, implementation costs, the entity's size, risk exposure, and the potential impact on services, systems, processes, and data integrity.

The core of this standard is therefore not merely the possession of formal documentation, but the genuine and practical implementation of cybersecurity measures based on knowledge of assets, risks, and threats, as well as the actual application of procedures in day-to-day operations. As emphasized in the Ministry of Digitization's Q&A guide, the key obligation of both key and important entities is to implement an ISMS encompassing regular risk assessment and decision-making regarding risk treatment, with technical and organizational measures tailored to the specific characteristics of the organization, including its size, the nature of the services provided, financial capacity, current technical knowledge, and current threats. Rather than imposing a universal set of safeguards, the regulations require solutions adapted to the individual needs of the specific entity. In this sense, the obligations of important entities are explicitly managerial rather than merely technical, since they require not only the implementation of security measures, but above all the building of organizational capability to maintain cybersecurity over time. This includes determining the entity's status, registration in the relevant register, connection to the S46 system, and implementation of the ISMS, while the Act also permits the use of external resources without relieving the organization of responsibility. Cybersecurity tasks may therefore be performed by internal structures or outsourced to external service providers, provided that effective execution and oversight are ensured. What remains essential is that the entity retains the capacity to coordinate, supervise, and hold accountable all actions taken in the cybersecurity domain, rather than merely purchasing security services. The detailed implications of this arrangement for organisational capability are discussed in Section 5 (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The conclusion to this section should be that an important entity must genuinely demonstrate the capacity to achieve and maintain a defined level of managerial and operational maturity in the area of cybersecurity. Merely fulfilling formal or legal requirements is not sufficient. What becomes essential is the actual implementation of effective risk management mechanisms, continuous improvement of procedures, and the building of organizational resilience to incidents. The status of an important entity thus entails the obligation to actively shape a security culture and to ensure the lasting, practical application of cybersecurity standards, which constitutes the essence of the logic of the NIS2 system and its Polish transposition.

4. State of research and research gap

Existing publications focus on the legal aspects of the NIS2 Directive and the placement of the new regulations within the EU legal system. These analyses organize the legal context, emphasizing the expansion of sectors, increased obligations in risk management, board accountability, and enforcement; however, they address to a limited degree the practical building of implementation capability in organizations (Teichmann, 2025; Vandezande, 2024).

A second group of publications focuses on practical aspects of NIS2 implementation and compliance obstacles, particularly identifying barriers such as resource constraints, competence limitations, and organizational specificity. For example, Mentzelou et al. (2025) present an analytical model of implementation difficulties without, however, addressing the specifics of national conditions or the differences between categories of entities subject to the Directive (Mentzelou et al. 2025).

A third area of research concerns cybersecurity governance, managerial accountability, and organizational resilience. It is emphasized that cybersecurity is becoming part of the organization's management system and managerial accountability, highlighting the importance of adaptation, inter-departmental collaboration, and the integration of technological and managerial resources. However, these analyses rarely refer directly to the requirements of the NIS2 Directive or the specifics of important entities (Galle, Vletter-van Dort, 2025; Dupont et al., 2023).

Institutional materials, such as the ENISA NIS2 Technical Implementation Guidance, have practical significance for implementing risk management, of a technical-operational nature, yet they do not explain the organizational costs, conditions, or barriers to implementation across different types of organizations (ENISA, 2025).

The Polish research context is less well explored. Legal and expert publications on cybersecurity for example, "Introduction to IT Security" (Securitum) is an expert publication of a technical and practical nature. Of key importance is the Ministry of Digitization document,

which explains implementation aspects and interprets the regulations in the context of the Polish transposition of NIS2 (Sajdak, 2023; Kowalski, 2023; Ministry of Digitization, 2026).

Based on the above considerations, a research gap emerges. First, most available publications on NIS2 focus on legal and compliance aspects, while organizational and managerial issues are relatively poorly described. Second, although analyses of implementation barriers, cybersecurity governance, and cyber resilience are appearing, they do not always refer directly to important entities, even though these are subject to similar requirements as key entities while often having limited resources, less formalized structures, and a smaller competence base. Third, there is a lack of detailed studies focusing on the Polish NIS2 implementation process following the amendments to the Act on the National Cybersecurity System. It therefore seems justified to shift the research focus from analysis of the regulations to examination of the most important challenges related to identification, organization, and operations, which are of key importance for the effective implementation of NIS2 by important entities.

5. Results: key challenges. the perspective of important entities

From the perspective of important entities, the implementation of NIS2 should be viewed not so much as a one-time adjustment to legal requirements, but as a new, continuous process one requiring a lasting linkage between regulatory obligations and the organization's actual mode of operation. In the Polish transposition, of particular significance is the fact that entry into the statutory regime is based on the entity's own self-identification, requiring it to relate its activities to Article 5 of the uKSC and to Annex 1 and Annex 2. Already at this stage, the organization must combine an analysis of requirements with detailed knowledge of its own organizational structure, business processes, resources, and ICT systems.

Further obligations arising from the Act extend beyond purely formal matters. According to the explanatory materials, adaptation to the requirements of the Act requires simultaneously: determining the entity's status, organizing internal accountability structures, implementing an information security management system, developing appropriate procedures, registering in the S46 system, and ensuring readiness to respond to incidents and cooperate with other institutions. For this reason, the key challenges for important entities should be analyzed from three complementary perspectives: identification, organizational, and operational. Such a division allows one to capture not merely the catalogue of obligations, but the conditions for their fulfillment within the organization (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026; UE L 333, 2022).

5.1. Identification Challenges

The first identified group of challenges faced by organizations are identification challenges. The organization must pose the following questions and attempt to find answers to them:

- is the Organization subject to the regime of the Act on the National Cybersecurity System? If so,
  - what extent do the provisions apply to it?
  - what specific implementation actions need to be planned?
  - what deadlines must be reached in the process?

The Polish implementation model is based on an active self-identification process on the organization side. As indicated in the Ministry of Digitization's materials, an entrepreneur who does not know whether they are subject to the national cybersecurity system should first establish their size, the types of activities carried out, the number of personnel employed, and the formal legal basis for conducting the activity, and then relate these findings to Article 5 of the Act and to the activities specified in Annex 1 and Annex 2 (Ministerstwo Cyfryzacji, 2026).

In this context, identification extends beyond a purely formal dimension and requires a close linking of legal criteria with the real structure and activities of the organization. According to the Ministry of Digitization document, the basis for assessment is not only registration data, but also financial statements, the number of employees, properly declared PKD (Polish Classification of Activities) codes, and official documents such as concessions, permits, or entries in registers of regulated activities. Additional complexity is introduced by the need to resolve whether, when determining the size of an enterprise, partner or affiliated entities should be taken into account. The explanatory materials emphasize that this is not merely an accounting matter, since it is also relevant whether those entities provide the same service and whether their information systems are functionally linked. Thus, the identification challenge consists not only in answering the question "am I subject to the Act?" but also "on what basis?", "to what extent?", and "taking into account what organizational relationships?" (Ministerstwo Cyfryzacji, 2026).

It is worth raising the open question here as to whether such a level of complexity in the identification process does not pose too great an organizational challenge for all organizations, especially the smaller ones or those with limited resources or competences?

A key aspect of the analyzed implementation phase is the precise determination of the substantive scope of organizational obligations, which includes the identification of services and information systems requiring coverage by further implementation procedures.

The Q&A document indicates that, following the phase of qualification of the entity's legal status, the legislator assumes the completion of another identification task: the designation of those information systems in which it will be necessary to implement an information security management system. It follows that the identification process is not limited to the legal

qualification of the enterprise but evolves toward functional qualification within which the organization is obliged to delineate the resources, processes, and systems relevant to the provision of the regulated services. This approach is consistent with the NIST concept, which treats cybersecurity as a process of shaping an organizational profile based on business requirements, acceptable risk levels, available resources, and the specifics of the organizational environment. In this context, identification constitutes a fundamental precondition for designing protective actions, being not only a preliminary legal act, but also a key element of the organization's strategic management process (Ministerstwo Cyfryzacji, 2026; NIST, 2018; NIST, 2026).

From the perspective of entities, the implementation deadlines are also of significant importance, they force the translation of identification findings into specific actions within a defined timeframe. In accordance with the Act, an application for entry in the register of key and important entities must be submitted within 6 months of the conditions for recognition as such an entity being met. The Ministry of Digitization document clarifies that other significant deadlines include:

- connection to the S46 system, and
- implementation of ISMS obligations within 12 months of the conditions for recognition as a key or important entity being met.

In this sense, identification challenges encompass not only the recognition of status itself but also the determination of the sequence of actions that must be planned on the organization's part. The S46 system itself does not yet constitute the essence of the identification challenges but is one of the first visible consequences of identification, a point of transition between the qualification phase and the organizational-operational phase (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

Challenges related to identification should be treated far more broadly than as a simple assignment of an entity to a given category. In the case of important entities, this process consists primarily in determining the scope of obligations, which requires establishing: regulatory status, sector of activity, type of activities carried out, company size, scope of services provided, and information systems, as well as indicating the key deadlines and actions initiating the next steps. Correctly completing this phase then enables the undertaking of organizational challenges, such as the allocation of responsibility, provision of appropriate resources, and creation of a compliance model, as well as operational challenges related to the day-to-day fulfillment of security requirements. Identification should therefore be regarded as a fundamental implementation phase, conditioning the course of the entire process, any errors made at this stage may negatively affect subsequent actions (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

Evidently, some tasks such as determining the type of activity carried out or the size of the company, can objectively be considered uncomplicated and requiring primarily formal analysis. However, other aspects, including establishing the organizational context or other aspects

related to the preparation of the ISMS, may pose a serious organizational challenge for entities, especially those with a complex structure or limited resources.

5.2. Organizational Challenges

The second category comprises organizational challenges, consisting in the need to create a model of organizational functioning that enables the genuine, continuous fulfillment of obligations, rather than merely their formal declaration. For at least some important entities, these challenges mean not so much the modification of already existing and mature cybersecurity structures as their construction from scratch, rationalization, or formal implementation. In this context, as mentioned above, NIS2 and the uKSC do not always introduce revolutionary changes in terms of the security standards themselves; however, they may constitute a significant turning point at the organizational level, especially for those organizations that have not previously regarded cybersecurity as a distinct managerial and operational function (Ministerstwo Cyfryzacji, 2026; Mentzelou et al., 2025).

The fundamental challenge stems from the very nature of the obligations defined by the Act. The provisions require an important entity to implement an information security management system in those information systems that have an impact on service delivery. Meaning the system must cover, among others: risk assessment, human resource protection, security and continuity assurance within the supply chain, constant monitoring, analysis of the effectiveness of applied technical and organizational solutions, and employee education. The legislator thus expects not the implementation of a single tool or procedure, but a holistic, durable organizational solution integrating managerial, technical, personnel, and relational aspects. In practice, the first organizational step is defining the internal accountability structure. The Ministry of Digitization materials indicate that the head of the entity not only approves the solutions developed, but is also responsible for the preparation, implementation, application, review, and control of the ISMS, plans an appropriate budget, delegates tasks and supervises their implementation, and promotes employee awareness of cybersecurity obligations. As a result, cybersecurity becomes embedded in the management structure of the organization as a whole. The literature emphasizes that proper cybersecurity management requires:

- clear division of responsibility,
- active communication within the organization,
- development of management competences, and
- integration of cybersecurity issues into the general enterprise management system (Dz.U. 2026, poz. 252; Galle, Vletter-van Dort, 2025; Ministerstwo Cyfryzacji, 2026).

One of the key organizational challenges is developing or acquiring appropriate executive competences. According to the Ministry of Digitization guidelines, cybersecurity tasks may be carried out in two ways:

- using internal teams, or
- entrusting some obligations to external service providers.

Outsourcing in the area of cybersecurity may cover only specific tasks, and the choice of the appropriate solution must be carefully considered to ensure the effective fulfillment of obligations. The regulations do not require the full transfer of security functions to internal structures, while at the same time not allowing outsourcing to be treated as a means of avoiding responsibility. Every organization must make a decision not only about building its own team, but also about which competences should remain in-house and which may be entrusted to external entities. In this regard, it is worth noting the approach presented in NIST, treating competence gaps and team potential as one type of organizational risk. NIST SP 1308 suggests that, depending on strategy, budget, risk level, and other available resources, an organization may consider hiring new employees, upskilling, reorganizing, or changing risk management methods. The foundation is an assessment of both internal team and external provider capabilities, incorporating these factors into decisions, and building a competence model tailored to the risk profile and scale of requirements. However, the decision to outsource cybersecurity functions carries its own set of organizational risks that important entities must manage. Dependence on a single external provider, commonly referred to as vendor lock-in, may limit the entity's ability to switch suppliers, renegotiate terms, or maintain operational continuity in the event of a provider failure or contract termination. Furthermore, standard service level agreements (SLAs) offered by security service providers are not always aligned with the specific reporting timelines and incident response obligations imposed by NIS2 and the uKSC, creating a risk of regulatory non-compliance that formally remains with the entity rather than the provider. Additional complexity arises in relation to data localization requirements under e.g. GDPR and the accessibility of systems and logs to competent cybersecurity authorities during audits or incident investigations. To mitigate these risks, important entities should ensure that outsourcing arrangements are governed by contractual provisions that explicitly address NIS2 and uKSC compliance obligations, define measurable performance indicators, and preserve the entity's right to audit, monitor, and terminate the engagement without compromising service continuity (Galle, Vlettervan Dort, 2025; Ministerstwo Cyfryzacji, 2026; NIST, 2026).

Additionally, it is worth bearing in mind that creating and maintaining an appropriate competence structure is associated with an increase in operational costs. The outcome of these actions, in accordance with the Act, should be an increase in awareness and organizational discipline. The Ministry of Digitization materials emphasize that documentation alone will not guarantee compliance if it is not applied in practice the organization should know its assets, risks, and threats, and procedures must be implemented, tested, and used. Employees should be regularly trained, and educational programs should cover both ISMS obligations and procedures, as well as specific examples of threats and incidents. In this way, organizational challenges are not limited merely to creating a security function, but also encompass

a transformation of the organization's approach to accountability, knowledge, and day-to-day practices and constitute one of the additional, permanent operational costs for enterprises (Galle, Vlettervan Dort, 2025; Ministerstwo Cyfryzacji, 2026; NIST, 2026).

The next aspect concerns the management of relations with external entities in the context of the ICT supply chain. Both the regulations and the Ministry of Digitization publications emphasize that ensuring security and continuity in the supply chain of ICT products, services, and processes is an integral part of the information security management system specifying that organizations should be aware of the structure of their supply chain, recognize risks associated with suppliers, define appropriate requirements, monitor vulnerabilities, and implement mitigation actions. In practice, the organizational challenge lies in ensuring that contracts and cooperation with suppliers are incorporated into the internal risk management system, rather than functioning outside managerial control (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026; NIST, 2018).

Concluding this part, it can be observed that the literature emphasizes that the problem discussed does not reduce to the formal compliance of organizations with the regulations, but may constitute a significant barrier to the organizational capability of entities particularly smaller ones. A lack of awareness, technical complexity, and financial constraints mutually reinforce one another, leading to weakened risk management and reduced operational resilience. It is particularly important to treat personnel shortages and limited resources not merely as a matter of headcount, but as a challenge requiring, inter alia, a well-considered configuration of competences, resource sharing, or the automation of repetitive tasks. This approach corresponds to the realities of important entities, which do not always have the capacity to build comprehensive cybersecurity teams, yet must ensure an appropriate capacity for oversight, coordination, and accountability for actions taken by employees, processes, and external partners. Thus, organizational challenges reduce to four fundamental questions:

- who bears responsibility?
- What competences are critical?
- Which tasks may be entrusted to external providers? and
- how to ensure that the implemented solutions function in practice?

This is where the greatest difficulties may arise for many organizations, namely, the translation of general statutory and industry security standards into specific roles, budgets, procedures, reporting lines, and supplier relationships. Consequently, organizational challenges constitute a key element linking the identification phase with the practical fulfillment of obligations (Galle, Vletter-van Dort, 2025; Mentzelou i in., 2025; NIST, 2026).

5.3. Operational Challenges

The third group comprises operational challenges, referring to difficulties associated with the ongoing fulfillment of the obligations defined in the Act in such a way as to not only meet regulatory requirements but also maintain the smooth operation of business processes and continuity of service provision. At this level, NIS2 and the uKSC exert the most direct impact on the organization, translating general statutory obligations into day-to-day activities such as monitoring, updating, documenting, reporting, communicating, responding, and cooperating with authorities and users. The legislator thereby also imposes a specific operational regime that may affect the organization's mode of operation in various ways (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The first dimension of the challenge is associated with the obligation to maintain continuous oversight of the information environment. Both the Act and the Ministry of Digitization materials indicate that the information system used to provide a service should be subject to continuous monitoring and the organization must analyze events that may constitute the cause or consequence of an incident. The Ministry's materials clarify that monitoring should cover, inter alia: traffic to and from the entity, system access, privileged accounts, critical configuration files, backups, security tool logs, and environmental events. In practice, this entails the need to maintain not only the technical capacity to record events, but also the capacity to interpret and prioritize them which may generate additional operational burdens (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The second dimension concerns incident management under time pressure and the need to make protective decisions that may disrupt the normal course of operations. The Ministry's materials indicate that serious incidents are reported via the S46 system, as a rule within 72 hours of their detection, together with information on the impact on the service, number of users affected, and remediation actions taken. In certain situations, further reporting obligations also arise such as an early warning, a progress report, or a final report. At the same time, the entity may be obliged to immediately limit certain technical activities, including temporarily restricting network traffic, if the protection of services and systems so requires. This means that the organization must simultaneously stabilize the operational situation, report the incident, and take decisions that may undermine current operational availability. The literature indicates that precisely operational disruptions, high reporting costs, and inadequate risk assessment are among the most significant challenges in this area. It is worth emphasizing that the potential costs associated with taking such actions, especially where they prove to be unjustified, may be particularly burdensome for the organization: leading, for example, to revenue loss, deterioration of client relations, reduced employee effectiveness, or the need to engage additional resources to restore system functionality. Accordingly, every decision to limit activities should be preceded by a thorough risk analysis and assessment of potential consequences, in order to avoid unnecessary costs and ensure the organization's operational effectiveness (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026; Mentzelou et al., 2025).

The next aspect concerns the ongoing updating of operational documentation and the continuous management of relationships with external entities. According to the Ministry's guidelines, an organization cannot limit itself to formal compliance, it should know its assets, risks, and potential threats, and should have procedures that are genuinely applied in day-to-day operations. The regulations impose an obligation to maintain documentation and records confirming the fulfillment of required activities. Additionally, an important entity is obliged to cooperate with relevant authorities, CSIRT teams, users, and suppliers, taking into account in its actions the consequences of recommendations, informing about significant events, and implementing remedial measures. From an operational perspective, this means that security becomes an integral element of day-to-day coordination, both internal and external, rather than merely a set of technical safeguards (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

The framing proposed in the literature on NIS2 implementation barriers appears apt: Mentzelou et al. indicate that operational disruptions, high reporting costs and inadequate risk assessment are among the most consequential effects of organizational pressure, absorbing the impact of earlier deficits in awareness, resources, and managerial capacity. This means that operational difficulties do not appear only at the end of the implementation process, they represent the point at which earlier identification and organizational shortcomings accumulate. NIST SP 1308 reinforces this perspective, indicating that cybersecurity management should be integrated with Enterprise Risk Management (ERM), staffing decisions, and operational planning, and that the organization should have the capacity for permanent monitoring and, where necessary, updating its risk profile and implementing corrective actions.

Consequently, the operational challenges of important entities can be viewed as difficulties associated with the day-to-day functioning of the organization under conditions of growing security requirements. They encompass the need to simultaneously maintain constant monitoring, report incidents, update systems, maintain documentation, and cooperate with supervisory institutions. While preserving operational continuity and the high quality of one's own services. It is precisely at this level that the regulations may generate the greatest tensions increasing coordination costs, slowing decision-making processes, amplifying administrative burdens, and forcing compromises between the level of security and operational efficiency. For this reason, operational challenges should be viewed not as the mere execution of statutory obligations but as a significant test of the organization's actual maturity in the area of cybersecurity (NIST, 2026; Mentzelou et al., 2025).

6. Discussion and conclusions

The analysis conducted indicates that the implementation of NIS2 requirements as expressed in the uKSC by important entities should not be framed solely as a challenge of formal-legal compliance, but as a process of building and maintaining organizational capabilities in the area of cybersecurity. Already the explanatory materials accompanying the amendment to the Act on the National Cybersecurity System indicate that the implementation of the new regulations will pose a particular challenge for the new key and important entities. This means that the regulatory burden does not reduce to the mere reading of obligations, but to the capacity to translate them into managerial, organizational, and operational practice. In this context, the distinction between identification, organizational, and operational challenges is of key importance. First, an important entity should independently determine its regulatory status, analyzing the scale and profile of its activities in relation to Article 5 of the Act and the relevant sectoral annexes. Second, the organization must create or formalize an internal system of accountability, competence, and oversight, including in the case of partial outsourcing of tasks to third parties. Third, the essential burden of regulatory implementation manifests at the operational level. Where obligations relating among other things reporting, monitoring, documentation, and cooperation with institutions should be seamlessly integrated with day-to-day organizational processes particularly in those organizations that had not previously focused on such activities (Dz.U. 2026, poz. 252; Ministerstwo Cyfryzacji, 2026).

Compared with existing studies on NIS2 and cybersecurity governance, which largely focus on legal analysis or generic implementation barriers, this paper shifts the perspective to the specific management challenges of important entities under the Polish transposition. By linking regulatory obligations with identification, organizational and operational capabilities, it offers a practice-oriented view that complements mainly doctrinal or technically driven contributions. The main contribution is the three-dimensional framework of identification, organizational and operational challenges, which integrates EU-level requirements with the concrete conditions faced by important entities in Poland. This framework can be used as a conceptual basis for assessing organizational readiness for NIS2 and for designing governance models, resource allocation and prioritization of cybersecurity investments in important entities (Teichmann, 2025; Vandezande, 2024; Mentzelou et al., 2025; Galle, Vletter-van Dort, 2025).

The conclusions of the analysis indicate that for many important entities, the provisions arising from the NIS2 Directive and the uKSC constitute not only a change of a regulatory nature but also an impulse to formalize the approach to cybersecurity at the organizational level. This phenomenon applies in particular to those institutions that had not previously possessed distinct security structures or had treated them merely as a supplement to the IT department. An important entity should therefore be understood not only as a legal concept, but as an organization from which the legislator expects the achievement of a defined level of maturity in cybersecurity management.

While a comprehensive cybersecurity maturity model goes beyond the scope of this paper, the framework proposed here suggests several baseline indicators that could serve as a starting point for assessing organizational readiness in important entities. These include:

- existence of a formally implemented ISMS covering key information systems,
- assignment of dedicated cybersecurity roles and responsibilities, like NIS2 coordinator or equivalent function,
- documented and tested incident response and reporting procedures aligned with the notification requirement, and
- evidence of regular cybersecurity training for management and staff.

The development of validated, sector-specific maturity indicators remains an important direction for future empirical research (Dz.U. 2026, poz. 252; ENISA, 2023; Ministerstwo Cyfryzacji, 2026; NIST, 2026).

The final conclusion is that the effectiveness of NIS2 implementation by important entities depends primarily on the capacity to combine the correct identification of obligations, the rational shaping of the implementation model, and the maintenance of operational efficiency under conditions of new requirements. It is at the intersection of these three dimensions that the fundamental management challenge emerges, as the ability to align legal expectations with organizational arrangements and day-to-day operations ultimately determines the maturity and resilience of the entity. From a research perspective, this justifies further analyses focused on practical models for fulfilling obligations, including support mechanisms for business in this process and the relationship between organizational maturity and the capacity to maintain operational compliance over the longer term. Future research should therefore validate this framework in selected sectors and compare important entities with key entities in terms of cybersecurity maturity and implementation costs. Quantitative studies could also develop operational indicators for organizational capabilities and workforce readiness, thereby moving beyond purely conceptual analysis.

References

1. Dacko-Pikiewicz, Z., Szczepańska-Woszczyna, K., Lis, M. (eds.) (2025). *Horyzonty sztucznej inteligencji a Przemysł 5.0.* Dąbrowa Górnicza: Akademia WSB.
2. Dupont, B., Shearing, C., Bernier, M., Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security, 132*, 103372. doi:10.1016/j.cose.2023.103372.
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE)

2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Dz.U. UE L 333 z 27.12.2022, p. 80.

4. ENISA (2023). *NIS Investments 2023. Cybersecurity Policy Assessment. European Union Agency for Cybersecurity,* listopad 2023. Download from: https://www.enisa.europa.eu/sites/default/files/publications/CSPA%20-%20NIS%20Investments%20-%202023.pdf, 10.04.2026.
5. ENISA (2025). *NIS2 Technical Implementation Guidance. European Union Agency for Cybersecurity,* czerwiec 2025. Download from: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf, 10.04.2026.
6. Galle, A., Vletter-van Dort, H. (2025). From cybersecurity to cyber resilience in the board room: key steps for supervisory board members and non-executives. *International Cybersecurity Law Review, 6*, pp. 221-237. doi:10.1365/s43439-025-00151-7
7. Hubbard, D., Seiersen, R. (2024). *Ryzyko w cyberbezpieczeństwie. Metody modelowania, pomiaru i szacowania ryzyka. Wydanie II*. Gliwice: Helion.
8. Kowalski, S. (2023). *Dyrektywa NIS2. Co to jest i jak ją wdrożyć w firmie*. Download from: https://mycompanypolska.pl/artykul/dyrektywa-nis2-co-to-jest-i-jak-ja-wdrozyc-w-firmie, 10.04.2026.
9. Mentzelou, K., Chountalas, P.T., Kitsios, F.C., Magoutas, A.I., Dasaklis, T.K. (2025). Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy, 5(4),* 97. doi:10.3390/jcp5040097
10. Ministerstwo Cyfryzacji (2026). Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa po nowelizacji PYTANIA I ODPOWIEDZI. Download from: https://www.gov.pl/attachment/4a661bd4-712c-4faf-8025-bcad437e5a29, 10.04.2026.
11. NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.* National Institute of Standards and Technology, 16 kwiecień 2018. Download from: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf, 10.04.2026.
12. NIST (2026). *NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide. NIST Special Publication 1308.* National Institute of Standards and Technology. Download from: https://www.nist.gov/publications/nist-cybersecurity-framework-20-cybersecurity-enterpriserisk-management-and-workforce -access date 10.04.2026
13. OWASP (2021). *OWASP Top 10: 2021. Open Worldwide Application Security Project*. Download from: https://owasp.org/Top10/2021, 10.04.2026.
14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U. UE L 119 z 4.5.2016, s. 1.

15. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011. Dz.U. UE L 333 z 27.12.2022, s. 1.
16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Dz.U. UE L 2024/1689 z 12.7.2024.
17. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności). Dz.U. UE L 2024/2847 z 20.11.2024.
18. Sajdak, M. (ed.) (2023/2024). *Wprowadzenie do bezpieczestwa IT. Tom 1 i Tom 2*. Kraków.
19. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus. *International Cybersecurity Law Review, 6*, pp. 207-220. doi:10.1365/s43439-025- 00154-4
20. Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Dz.U. 2026, poz. 252.
21. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review, 52,* 105890. doi:10.1016/j.clsr.2023.105890